

**AFFIDAVIT IN SUPPORT OF AN APPLICATION  
FOR AN ANTICIPATORY SEARCH WARRANT**

I, Jonathan A. Duquette, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION**

1. I am a Task Force Officer with the Federal Bureau of Investigation (FBI). I have been in this position since June 2015, and I have been a Task Force Officer in FBI's Boston Division since January 2018. I am also a Border Patrol Agent with the U.S. Border Patrol and have been in this position since December 2009. In my career, I have utilized various investigative tools and techniques, to include the use of search warrants.

2. I am an investigative or law enforcement officer of the United States within the meaning of Section 2510(7) of Title 18, United States Code, and am empowered by law to conduct investigations of and to make arrests for federal criminal offenses. I also am a "federal law enforcement officer" within the meaning of Rule 41 of the Federal Rules of Criminal Procedure.

3. I make this affidavit in support of an application for an anticipatory search warrant under Federal Rule of Criminal Procedure 41(b)(1), to search for and seize contraband, evidence, fruits, and/or instrumentalities of 18 U.S.C. § 2252A(a)(2)(A) (receipt and attempted receipt of child pornography) and § 2252A(a)(5)(B) (possession and attempted possession of child pornography). Specifically, I seek authorization to search for and seize the items more fully set forth in **Attachment B** of this affidavit.

4. These items are believed to be contained in information associated with the Mega LTD (“Mega”) account andrewhazelton542@gmail.com<sup>1</sup>—respectively, the “Subject Account Information” and the “Subject Account.” The Subject Account Information is currently believed to be stored on Mega servers in New Zealand, but is anticipated to be downloaded to computer media in the possession of the FBI located in the District of Maine, as further described in **Attachment A.**

5. The facts set forth in this affidavit are based upon my investigation, my training and experience, and information I have received from other law enforcement officers and witnesses. Because I am submitting this affidavit for the limited purpose of obtaining a search warrant, I have set forth only the facts that I believe are sufficient to establish probable cause that contraband, evidence, fruits, and/or instrumentalities of violations of the Subject Offenses will be located in the Subject Account Information at the time the warrant is executed.

### **BACKGROUND ON MEGA**

6. In my training, experience, and research, I have learned that Mega is a company that provides file-hosting and communications services to the public, through the website Mega.nz. Mega is headquartered at Level 21, Huawei Centre, 120 Albert Street, Auckland, New Zealand. On information and belief, Mega’s computer servers are located in New Zealand, and Mega does not have offices or employees in the United States.

7. A Mega user can sign up for an account with a valid email address, which becomes the user’s Mega username. Mega provides users with a certain amount of free data

---

<sup>1</sup> As described in Paragraph 7, a Mega username takes the form of the full email address submitted by the user to create the account.

storage; if a user wants more storage, the user can pay for it. Users can access Mega through the internet from most major devices and platforms, from anywhere in the world. For example, a user may take a photo with their cell phone, upload that photo to Mega, and then delete the photo from their cell phone. The photo now resides on Mega's servers. The user can then access their Mega account from a different device, such as a desktop computer, and download the photo to that computer.

8. A Mega user can designate a special folder (or folders) on their computer, which Mega synchronizes with the user's account. As a result, that same folder, with the same contents, will appear on both the user's computer and their Mega account. Files placed in that folder are accessible through Mega's website, as well as its mobile-phone applications.

9. In addition, Mega users can share files with other people by sending web links, which give access to the particular shared files.

10. Another feature of Mega is "MegaChat," which allows users to exchange messages and have audio, video and group chats.

11. According to Mega, data associated with a Mega account is stored on Mega's servers in an encrypted format. Data is also transmitted in an encrypted format between Mega's servers and users' devices. Messages between Mega users are also transmitted in an encrypted format within Mega's secure server network. Because data is encrypted at all steps, the risk of files or messages being intercepted is minimal.

12. Mega's server architecture means that data is encrypted in a way that makes it generally inaccessible to Mega. Data is encrypted on the client side using an encryption key to which Mega does not have access. This means that, barring exceptional circumstances, Mega

does not have the technical ability to decrypt user's files or messages and, as a result, Mega is unable to provide data in a usable format to third parties. Mega also is unable to conduct data recovery. If a user forgets their password, Mega cannot recover that user's data.

13. As explained herein, the Subject Account Information may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion. This information can indicate who used or controlled the Subject Account. For example, communications, contacts lists, and files sent or uploaded (and the metadata associated with the foregoing, such as date and time) may indicate who used or controlled the Subject Account at a relevant time. The information may also reveal the identity of other victims and the underlying time frames in which they were victimized (e.g., folders with victim data and the metadata associated with file transfers). Additionally, stored electronic data may provide relevant insight into the Subject Account owner's state of mind as it relates to the offenses under investigation. For example, information in the Subject Account may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime) or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

#### **PROBABLE CAUSE**

14. On April 28, 2021, I obtained search warrants for 25 Elmwood Street in Portland, Maine, and for the person of Andrew Hazelton. A copy of my affidavit in support of the warrants is attached as Exhibit 1 and incorporated here.

15. On April 29, 2021, at about 11:20 a.m., other FBI investigators and I executed the search warrants at 25 Elmwood Street in Portland. We encountered Andrew Hazelton just after he left the residence.

16. I informed Hazelton that we had search warrants for his person and his residence. Special Agent Kurt Ormberg took a mobile phone from Hazelton's left front pants pocket and handed it to me. The phone was later identified as a Samsung Galaxy S21 5G smartphone. The phone had been named "Andrew's S21."

17. The Samsung phone was locked when it was retrieved from Hazelton. I informed him that the search warrant permitted us to place his fingers on the phone to unlock it. After initially refusing to do so, he eventually placed one of his thumbs on the phone and it unlocked.

18. An analysis of the phone on-scene revealed a folder named "1488" in the Gallery application of the phone. The 1488 folder contained many video files. Among the files were dozens that depicted minors engaging in sexually explicit conduct. One such video had the file name 2020-08-05 20.36.19.mp4. The video, which was 14 seconds long, depicted a young girl, approximately six or seven years old, holding an adult male penis in her right hand. The girl then performed oral sex on the male while the male patted her head. The same girl was depicted in at least two other videos that were in the same folder.

19. The file path for the video described in Paragraph 18, as revealed by looking at the "Details" entry for the file, was /internal storage/MEGA/MEGA Downloads/1488. A random selection of five videos that appeared to portray minors engaged in sexually explicit conduct showed the same file path.

20. The Samsung phone has the Mega application installed. I attempted to open the application, but the application was separately protected requiring Hazelton's fingerprint or a PIN to unlock the application.

21. While agents executed the search warrant at 25 Elmwood Street in Portland, they located a powered-on desktop computer in Hazelton's bedroom. A random-access memory (RAM) extraction identified several alphanumeric combinations consistent with passwords.

22. On May 11, 2021, I contacted Mega utilizing the email address abuse@mega.nz inquiring how to identify an account. While waiting for a response I began researching Mega and located a link to log into an account utilizing an email address. I attempted to log in utilizing the known email address for Hazelton of andrewhazelton542@gmail.com and tried several passwords found on Hazelton's electronic devices. On the second attempt, utilizing an alphanumeric combination located in the computer RAM, the account appeared to begin to load. I observed the phrase "decrypting data" and closed the browser before any data was displayed.

23. Shortly thereafter, I received notification from Mega that they have a zero-tolerance policy involving Child Sexual Abuse Material and provided account information for Hazelton's Mega account tied to andrewhazelton542@gmail.com. The information indicates Hazelton has nine active public links. The account has three folders holding 34015 files containing 53690464502 bytes (53.69 GB) of data.

24. Additional review of the data provided by Mega indicated the account was opened on September 1, 2014. The last active session for an Android device was April 28, 2021, at 8:31:42 p.m. (Eastern Standard Time). On June 9, 2020, the account password was changed using IP address 142.105.197.8. Information from Charter Communications on the listed IP

address indicated the subscriber for that IP address during that time was registered to Andrew Hazelton at 25 Elmwood Street in Portland, Maine. The IP address captured during the creation of the Android device was 174.242.66.176 port 3571, which was determined to belong to Verizon Wireless. Records from Verizon Wireless indicated the Verizon telephone number utilizing that port on February 12, 2021 at 10:01:07 pm (EST) was 978-799-7087. The subscriber for that telephone number is John Hazelton of Westford, Massachusetts, Andrew Hazelton's father, and is assigned to Hazelton's Samsung Galaxy S21.

25. Three additional logins by the Android device in February, March, and April of 2021 utilized the Verizon Wireless network. The IP address was captured by Mega during the logins. Records from Verizon Wireless identified the target telephone number assigned the IPv6 address during the logins as 978-799-7087, which as stated in paragraph 24, is assigned to Hazelton's Samsung Galaxy S21.

26. Based on the foregoing, I submit that probable cause exists to believe that Andrew Hazelton used the Subject Account—including its encrypted features and its foreign location—to possess images of child pornography that he had obtained via the internet.

27. The information in the Subject Account is currently believed to be stored on Mega servers located in New Zealand. It is my understanding that the Fourth Amendment's warrant requirement generally does not apply to locations outside the territorial jurisdiction of the United States, *see United States v. Stokes*, 726 F.3d 880, 890–93 (7th Cir. 2013), and that a warrant issued under Federal Rule of Criminal Procedure 41 would not authorize the search of a server located in New Zealand under these circumstances. *See also United States v. Verdugo-Urquidez*, 494 U.S. 259, 274 (1990) (describing a warrant issued by a United States magistrate as

“a dead letter outside the United States”). Therefore, I seek this warrant out of an abundance of caution, to be certain that an examination of information from the Subject Account (i.e., the Subject Account Information) downloaded to computer media in the possession of the FBI located in the District of Maine will comply with the Fourth Amendment and other applicable laws.

### **CONDITION REQUIRED PRIOR TO EXECUTION**

28. The FBI plans on accessing the Subject Account using the known credentials; if such access is successful, the FBI intends to use Mega’s data transfer tools to download the account’s information onto computer media in the possession of the FBI, located in the District of Maine. The downloaded information (i.e., the Subject Account Information) may include, but is not limited to, files, communications and contact lists associated with the Subject Account.

29. I am seeking permission to search the Subject Account Information following the triggering event of the download of said information by the FBI into the District of Maine, as described in **Attachment A**, and to seize the items and information described in **Attachment B**.

30. *Manner of Execution.* Because this warrant seeks permission only to examine information on computer media in law enforcement’s possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

### **CONCLUSION**

31. Based on the information described above, I respectfully submit there is probable cause to believe that contraband, evidence, fruits, and/or instrumentalities of violations of the

Subject Offenses, specifically those items more fully set forth in **Attachment B**, are currently located in the Subject Account, and will be located in the Subject Account Information in the District of Maine at the time the warrant is executed.



Jonathan A. Duquette  
Task Force Officer  
Federal Bureau of Investigation

Sworn to telephonically and signed  
electronically in accordance with the  
requirements of Rule 4.1 of the Federal Rules  
of Criminal Procedure

Date: Jun 30 2021

City and state: Portland, ME



*Judge's signature*  
John H. Rich III, U.S. Magistrate Judge  
*Printed name and title*